FIREWALLS A LA VANGUARDIA

Forero Gandur, Jhonatan Wadin
Especialización en Seguridad Informática, Universidad Piloto de Colombia
Bogotá, Colombia
jhonatan0318@hotmail.com

Abstract*—The tool or information system that controls access and flow of network traffic also prevents unauthorized access to a computer or a computer network from another network that seeks to make an intrusion is known in the field of computer security as Firewall access. This tool allows or denies if the connection is established or not from another network, the importance of this is that by authorizing its use, detect or Redirect a connection without informing the sender. That is why for organizations is of vital importance to have kinds of solutions in order to prevent attacks from other networks as well stay clear unauthorized such as spies, hackers, crackers among other users.*

Key words*—Firewall, unauthorized Access, system security, policies.*

Resumen*—La herramienta o sistema de información que controla el acceso y el flujo de tráfico de red que además impide el acceso no autorizado a un computador o a una red de computadores desde otra red que pretende realizar una intrusión es denominada en el ámbito de seguridad informática como Firewall. Esta herramienta niega o permite que desde otra red se establezca una conexión o no se logre, la importancia de esta radica en que a través de su uso se autorice, detecte o se re-direccione una conexión sin informar al emisor. Es por esto que para las organizaciones es de vital importancia contar con este tipo de soluciones con el fin de evitar ataques desde otras redes pues así mantienen al margen a los usuarios no autorizados tales como espías, hackers, crackers entre otros.*

Índice de Términos*—Firewall, acceso no autorizado, seguridad informática, políticas.*

I. INTRODUCCIÓN

En la actualidad las organizaciones comprenden la relevancia de proteger la información, pues este es considerado como su recurso intangible más preciado debido a que esta se encuentra expuesta a personas mal intencionadas, gracias a los frecuentes intentos de intervención en las redes internas y/o externas se genera la necesidad de protegerlas por medio de Firewalls que controlen el acceso o lo denieguen.

El deber de las organizaciones con respecto a este recurso es asegurar la integridad, disponibilidad y confidencialidad pues no solo basta con conservarla sino que esta no debe ser alterada e intervenida, adicional se debe prever el acceso a esta en tiempo y forma para las usuarios interesados y aún más importante se debe asegurar que no será vociferada o expuesta a personal no autorizado.

Dado que la reputación organizacional es un valor fundamental para cualquier empresa dentro del mercado es mucho más seguro invertir en estrategias de prevención para la seguridad de la información que evidenciar una vulnerabilidad en la infraestructura organizacional, pues se manifiesta en riesgos de pérdida de clientes, prospectos y con seguridad se generan mayores gastos.

En consecuencia con lo anteriormente mencionado la tendencia de los Firewalls para las organizaciones se verá encaminada a la exploración de aplicaciones y políticas de control detalladas.

II. ANTECEDENTES

Antes de hablar de Firewalls debemos remontarnos al nacimiento de la INTERNET, este gran avance surge como la Red de Agencia de Proyectos de Investigación Avanzada (ARPANET) hasta ese entonces tan sólo era una pequeña comunidad cerrada donde todos se conocían entre sí, pero luego el dos de noviembre de 1988 Peter Yee en el Centro de Investigación Ames de la NASA informa a la comunidad por medio de correo electrónico que han sido atacados por un virus llamado Gusano Morris y es ahí cuando los creadores y organizaciones

afiliadas se percatan de que la red no era tan cerrada ni tan segura como ellos pensaban. A partir de este momento los investigadores comienzan a compartir información sobre sus prácticas con el fin de evitar futuras intrusiones. Algunos de los resultados de esta perturbación fue el aumento en las listas de correo dedicado a la seguridad y el seguimiento de errores. Gracias al Gusano Morris y demás incidentes que se presentaron en aquella época es que las personas empiezan a preocuparse por asegurar la red y a tomar conciencia por la protección de la información, en este punto se habla por primera vez del surgimiento de una herramienta que proteja a las redes de intrusiones desde otras redes.

III. HISTORIA

El término Firewall o cortafuegos no se originó con la Internet, de hecho los cortafuegos son barreras para el fuego que contienen un incendio hasta que los bomberos lleguen a apagarlo, para la industria automotriz se considera cortafuegos a una lámina que separa el compartimiento de los pasajeros con el motor, es decir que en tecnología llamamos Firewall o cortafuegos a un dispositivo o sistema de información que restringe el acceso entre dos o más redes [1].

Como se mencionó antes la necesidad del uso de Firewalls se debe al hecho de restringir el acceso entre redes con internet y otras redes en la zona desmilitarizada (DMZ) usando políticas de seguridad, esto se debió a que en los años 80’s la expansión de las redes militares y académicas dieron como resultado lo que hoy conocemos como Internet, asimismo la popularidad de los primeros computadores hicieron de este avance un objetivo fácil para la comunidad de Hackers nacientes.

A continuación se describirán las diferentes generaciones que han marcado la evolución de los Firewalls [2].

- Primera generación – Filtro de paquetes: La tecnología se dio a conocer en diciembre de 1988, fruto de la investigación de Bill Cheswick y Steve Bellovin de AT&T quienes propusieron un modelo de filtrado de paquetes donde se evalúa un conjunto de protocolos TCP/IP, esto quiere decir que se restringe el tráfico basándose en las IPs de origen, destino y a través de la puerta del servicio (Puerto).

- Segunda generación – Filtros de sesión Estado: Se conocen en la década de los 90`s por los laboratorios Bell y fueron llamados cortafuegos circuito. Estos tomaron las restricciones de los Firewalls que se tenían en la primera generación y adicionalmente a eso agregaron restricción de tráfico a principios de conexiones, el tráfico de paquetes que se inició desde la red protegida y restringía los paquetes que tenían número de secuencia correcta. Estos cortafuegos guardan el estado de las conexiones y filtros basados en ese estado, los cuales son conocidos como: NUEVO para nuevas conexiones, ESTABLECIDO para conexiones establecidas y RELACIONADO para las conexiones a otros existentes relacionados.

- Tercera Generación - Application Gateway: Fue esta la generación que lanzó el primer producto comercial el 13 de junio de 1991 y se hizo popular en los años 90. Se conoce con este nombre por la aplicación del concepto de representación y control de acceso en un solo dispositivo, es decir, es capaz de recibir un sistema de conexión, protocolos de decodificación en la capa de aplicación e interceptar la comunicación entre cliente / servidor para así aplicar las reglas de acceso. Se caracteriza porque implementó todas las reglas de las anteriores generaciones, restringió el acceso FTP a los usuarios anónimos a portales de entretenimiento y a protocolos desconocidos en el puerto 443.

- Cuarta Generación y posterior: Se consolida como una solución para redes de comunicación TCP / IP para inspeccionar paquetes y tráfico de datos en base a las características de cada aplicación, la información asociada con todas las capas del modelo OSI y el estado de las conexiones activas y las sesiones, prevención de

intrusiones con el propósito de identificar el abuso de los protocolos TCP / IP, inspección profunda de paquetes donde se combina la inspección de estado con las técnicas de los dispositivos IPS.

- Desde la década de 2000, la tecnología Firewall se ha mejorado para también ser aplicado en estaciones de trabajo y ordenadores domésticos, además de la aparición de soluciones Firewall dedicado a servidores y aplicaciones específicas o incluso los usuarios.

IV. RIESGOS EN LAS REDES INFORMÁTICAS

El riesgo en las redes de una organización puede ser visto desde tres puntos de vista:

- Infraestructura: Se hace refiere a el hardware.
- Lógico: Asociado a información, sistemas de información y software.
- Factor humano: Este deriva del mal uso de los dos anteriores.

Pero adicionalmente a esto existen los ataques intencionados o dirigidos para los cuales se usa de manera incorrecta la tecnología con la finalidad de explotar vulnerabilidades.

Podemos decir que el riesgo aumenta con el uso de herramientas y aplicaciones que no son correctamente gestionadas, configuradas o por su constante cambio, esto causa que existan vulnerabilidades a las que se exponen las organizaciones.

Es por esto que es tan importante que se dé cumplimiento a las medidas de aseguramiento, se haga mantenimiento y se realicen planes de continuidad del negocio.

V. CONTROLES EN LAS REDES INFORMÁTICAS

Cuando hablamos de controles debemos decir que son las acciones que se toman para mitigar el riesgo, estos controles o aseguramiento pueden abordarse desde los tres puntos de vistas anteriormente mencionados.

- Infraestructura: las medidas para este ítem son de carácter técnico, es decir la implementación de procedimientos de control de accesos no autorizados a recursos informáticos, estos pueden ser clasificados como controles de acceso físico, acceso a los equipos de cómputo, almacenamientos en medios removibles o tarjetas de identificación.

- Lógico: las medidas deben estar enfocadas en proteger los datos con el fin de garantizar el acceso solo a los usuarios que lo requieran. Mencionaremos algunas de estas medidas control de acceso lógico de usuarios, creación de perfiles, privilegios, gestión de contraseñas, control de acceso a la red interna, segregación de funciones, herramientas de control de malware, respaldo de base de datos, entre otros.

- Factor humano: las medidas que deben ser implementadas para este nivel son de tipo procedimental, en el marco de la regulación y concientización. Como es sabido las personas son el eslabón más débil de la seguridad y es por esto que debemos incluir definición de políticas de seguridad, acuerdos de niveles de servicios con terceros, gestión antes, durante y después de finalizado el contrato, capacitación en seguridad informática, cumplimiento de la legislación, por mencionar algunos.

Para este artículo nos enfocaremos en los controles lógicos donde nos centraremos en el acceso a las redes internas con el uso de firewalls.

VI. USO CONTEMPORÁNEO DEL FIREWALL

Actualmente para la mayoría de las organizaciones los Firewalls son la primera línea de defensa contra las amenazas de Internet para proteger su información, pues comprenden que esta es uno de los recursos más preciados.

Figura 1. – Ejemplo firewall. Disponible en http://uits.arizona.edu/services/firewalls

Por lo general en las implementaciones el Firewall actúa como un vigilante, pues permite únicamente las conexiones desde otras redes definidas por la empresa, en esencia el proceso consiste en coordinar reglas que contienen una IP de origen, destino y un servicio o puerto. De tal modo que las empresas han adoptado un modelo de arquitectura donde se aíslan de la red interna los servidores con acceso a Internet en una DMZ, es decir que, los equipos de cómputo no pueden acceder a estos servidores con servicios web a menos que el Firewall lo permita mediante el uso de reglas.

Basándonos en las configuraciones típicas de las organizaciones es evidente notar que el Firewall aún no ofrece protección en la capa de aplicación que es donde gran parte de las amenazas de seguridad se encuentran, es por eso que el Firewall es efectivo en el control de conexiones y que por tal razón es necesario usar herramientas que apoyen específicamente en el control de aplicaciones y amenazas de malware, por ende se han diseñado Firewalls con un propósito determinado por ejemplo Firewalls para la vigilancia del tráfico saliente (Proxy), Inspección del contenido de la capa de aplicación (Inspección de paquetes), Firewalls para aplicaciones web (WAF),Implementaciones de Firewalls virtuales (VS) [3].

Como lo hemos mencionado en varias oportunidades el firewall tiene como beneficios:

- Optimización del acceso al computador, Internet o DMZs de la empresa.
- Administra los accesos de la red privada hacia Internet, centralizando los accesos y controlando la seguridad.
- Protección de la información privada de la empresa y sus clientes.
- Protección ante intrusos externos.

Sin embargo, debemos tener en cuenta que los firewalls no protegen conexiones que no pasan a través de él, lo que significa que puede ser una conexión SLIP o PPP hacia internet o un sitio FTP expuesto por algún cliente.

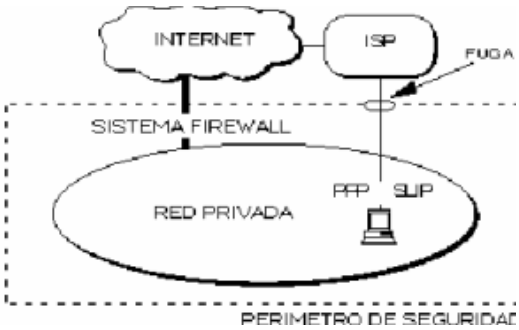

Figura 2. –Ejemplo de conexión que no pasa a través del firewall. Disponible enhttp://www.monografias.com/trabajos3/firewalls/firewalls.shtml

Otra de las externalidades negativas que afectan el buen rendimiento de los Firewalls es que no pueden proteger contra ataques o amenazas de usuarios corporativos con malas intenciones que puedan tomar la información y copiarla en un dispositivo de almacenamiento externo o de ataques de ingeniería social que pueden ser internos o externos.

Adicionalmente a esto existen técnicas de evasión como las que mencionaremos a continuación, las cuales son ofrecidas por la Organización NMAP: fragmentar los paquetes, utilizar el MTU (Maximum Transmission Unit) especificado, sondeo con señuelos, falsificar la dirección de origen, utilizar la interfaz especificada, falsificar el puerto de origen, añadir datos aleatorios a los paquetes enviados, establecer el campo de tiempo de vida de la cabecera IP, mezclar aleatoriamente la lista de equipos a sondear, adulterar la dirección MAC, enviar paquetes con sumas de comprobación

TCP/UDP erróneas. Todas estas técnicas de evasión son producto de una mala configuración o un descuido en los firewalls [4].

VII. TENDENCIA

En la actualidad la complejidad de la redes ha aumentado vertiginosamente ya que los empleados de las organizaciones tienen fácil acceso a múltiples aplicaciones en internet desde sus dispositivos móviles, generalmente no se tiene en cuenta los riegos para el negocio y para la seguridad por lo que se puede ver afectada el uso de la información sensible por las vulnerabilidades expuestas de la aplicaciones.

Es por esto que debemos centrarnos en las tres funciones fundamentales para las que está diseñado el firewall.

- Operar como el núcleo de la infraestructura de seguridad de la red.
- Actuar como un punto de control de acceso para todo el tráfico, permitiendo o denegando el tráfico en la red en función de las políticas.
- Eliminar el riesgo de lo “desconocido” usando un modelo de control positivo que se limita a establecer una estrategia del tipo “permitir lo que se desea y denegar implícitamente todo lo demás [5].

Actualmente las técnicas de evasión basadas en el salto de puertos, el uso de puertos no estándar y el uso del cifrado son algunas de las formas mediante las cuales las aplicaciones se han vuelto más accesibles. Estos mismos procedimientos también son usados por los atacantes cibernéticos de manera directa o indirecta.

Con el fin de dar solución a estos desafíos los fabricantes de firewalls están rediseñando la forma en que se identifica y controla el tráfico, pues ya no solo validan IPs y puertos sino se están centrando en las aplicaciones. Existen dos razones para este interés: primera, las amenazas relacionadas a las aplicaciones pueden evadir los firewall basados en IPs y puertos. La otra razón se refiere a que el firewall es un punto común donde fluye el tráfico de las organizaciones y es donde se aplican políticas de control de acceso.

Basados en lo anterior las nuevas soluciones de firewall deberán ser una herramienta donde se encuentren integrados controles de aplicaciones, usuarios, malware, inspección de paquetes a profundidad y protección contra amenazas desconocidas.

VIII. CONCLUSIONES

Como hemos visto a lo largo de este articulo los firewalls han sido y siguen siendo una herramienta importante para las organizaciones pues garantiza la disponibilidad, integridad y confidencialidad de la información considerada sensible ya que es una solución que garantiza el acceso a usuarios permitidos y rechaza aquellos que no los son permitiendo de esta manera detectar posibles violaciones de la seguridad informática y de esta manera tomar contramedidas para corregir estas vulnerabilidades identificadas.

Debe ser de carácter obligatorio que las organizaciones generen sensibilizaciones periódicas en el área de seguridad informática en donde se dé a conocer la importancia de la seguridad informática y se instruya en los principios básicos, esto con el fin de sensibilizar a los funcionarios y generar cultura en este ámbito,dado que su naturaleza impredecible, es el personal o recurso humano pues es el más crítico para las organizaciones.

Teniendo en cuenta la tendencia de los firewalls están en la capacidad de brindar a las organizaciones un equilibrio entre seguridad y maximizar la productividad comercial, pues se proyectan como herramientas robustas que puedan identificar intrusiones y detenerlas garantizando de esta manera que las organizaciones cumplan con sus objetivos comerciales.

Si bien es sabido que los firewalls no están en la capacidad de proteger a las empresas contra ataques de ingeniería social, usuarios mal intencionados o conexiones que no se establezcan a través de ellos, estos contribuyen en la mitigación del riesgo de

exponer la información en las redes internas o externas de las organizaciones.

IX. BIBLIOGRAFÍA

[1] (The Internet Protocol Journal) F. Avolio. (1999, Junio). Firewalls and Internet Security. Cisco [Web]. Volume (2), Nº 2. Available:http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html

[2] W. Cheswick. (2003, Abril). Firewalls and Internet security: repelling the wily hacker (2nd ed.) [Online]. Available: https://books.google.com.co/books?id=_ZqIh0IbcrgC&lpg=PA142&dq=Firewalls+and+Internet+Security,+by+Cheswick+et+al.&pg=PA176&hl=es#v=onepage&q=Firewalls%20and%20Internet%20Security%2C%20by%20Cheswick%20et%20al.&f=false

[3] A. Sastry. (2012, Noviembre). Implementación de firewall para nuevos tipos de ataques. [Online]. Available: http://searchdatacenter.techtarget.com/es/consejo/Implementacion-de-firewall-para-nuevos-tipos-de-ataques

[4] G. Lyon. (2011). Nmap Network Scanning [Online]. Available: http://nmap.org/book/toc.html

[5] 10 cosas que su próximo firewall debe hacer, Palo Alto Networks, Santa Clara, CA, 2013.